ABSTRACT OF THE DISCLOSURE

A method and system are disclosed that provide a significant improvement for securely selecting a subset of available cryptographic functionality in a system. This is implemented by using the highest level of cryptography available in a system to encrypt the system initialization data used to select, enable, disable, or configure cryptographic features in a crypto chip. The system decrypts the encrypted data by momentarily fully enabling the crypto chip during the boot process, and using a known, system-unique, and fixed seed to generate the private key to use for decryption. The seed used is the system's MAC address (L2 LAN address – medium access control). Alternatively, the system could include a one-time use decryption-only algorithm in the boot strap code itself.